ICANN org Urgent Requests Proposed Language

Rationale Paper

Isabelle Colas-Adeshina
28 August 2025

ICANN

TABLE OF CONTENTS

Background

The EPDP Phase 1 Recommendation 18 (Rec 18) anticipated **"a separate timeline for** responses to **urgent requests for lawful disclosure of non-public registration data"** and indicated that the response time and criteria would be established during implementation. The relevant section reads that a:

> ***"separate timeline of [less than X business days]*** *will be considered for the response to 'Urgent' Reasonable Disclosure Requests, those Requests for which evidence is supplied to show an immediate need for disclosure [time frame to be finalized and criteria set for Urgent requests during implementation]."*

Accordingly, ICANN org worked with the Implementation Review Team (IRT) to develop the following draft policy language for public comment:

> **Section 10.6:** *For Urgent Requests for Lawful Disclosure, Registrar and Registry Operator MUST acknowledge and respond without undue delay, but no more than* ***two (2) business days*** *from receipt. If responding to an Urgent Request for Lawful Disclosure is complex, or a large number of requests are received by Registrar or Registry Operator, Registrar or Registry Operator MAY extend the time for response* ***up to an additional one (1) business day from the date of receipt*** *of the Urgent Request for Lawful Disclosure, provided Registrar or Registry Operator provides notice to the requestor within the initial* ***two (2) business day period*** *and explains the need for an extension of time.*

ICANN org reviewed input from the public comment proceeding with the IRT, in light of concerns expressed that the language in 10.6 failed to implement expedited timeframes consistent with the urgency required to respond to urgent requests. On 20 January 2023, ICANN org subsequently proposed revised language in 10.6 in response to this feedback:

> ***Section 10.6****. For Urgent Requests for Lawful Disclosure, Registrar and Registry Operator* ***MUST acknowledge and respond without undue delay, but no more than 24 hours from receipt****. If responding to an Urgent Request for Lawful Disclosure is complex, or a large number are received by Registrar or Registry Operator, it* ***MAY extend*** *the time for response up to* ***an additional one (1) business day*** *from the date of receipt of the Urgent Request for Lawful Disclosure, provided it gives* ***notice to the requestor within the initial 24 hour period and explains the need for an extension of time.***

Here, ICANN org noted for the IRT the understanding "*that the 24-hour response time accurately reflects the intent of the EPDP policy recommendations, particularly in cases where urgent requests rise to the level of emergencies and are made to prevent harm to individuals or critical infrastructure, such as those related to the threat to life, human life and child exploitation.*"

In subsequent IRT discussions regarding Urgent Requests, some members opposed the 24-hour timeframe. As a result, the IRT held a set of dedicated meetings on this topic to reach a compromise that incorporated the notice of receipt within 24 hours while also allowing for an extended period to handle complex requests effectively. The following language was proposed on 24 July 2023:

> ***Section 10.6*** *...MUST respond, as defined in Section 10.7, without undue delay,* ***generally ./within 24 hours of receipt.***
>
> ***Section 10.6.1*** *If Registrar or Registry Operator cannot respond to an Urgent Request for Lawful Disclosure within 24 hours, it MUST notify the requestor* ***within 24 hours of receipt*** *of an Urgent Request for Lawful Disclosure of the need for an extension to respond…* ***which cannot exceed two (2) business days from the time of the initial receipt of the request.***
>
> ***Section 10.6.2*** *… if responding to an Urgent Request for Lawful Disclosure is complex, or a large number of requests are received by Registrar or Registry Operator,* ***it MAY extend the time for response up to an additional one (1) business day…***

The GAC did not agree with the suggested compromise language and in its 23 August 2023 correspondence to the ICANN Board, asked it to *"carefully review the proposed implementation of this particular issue and consider next steps that would achieve an outcome that better meets the public safety considerations posed by urgent requests."* The GAC also advocated for a **reduction of the maximum three-business-day turnaround** for urgent requests for the lawful disclosure of gTLD non-public registration data, emphasizing the need for a more timely response to imminent threats to lives and infrastructure, and requested the ICANN Board to review the policy ahead of publication.

As a result, the publication of the Registration Data Policy was temporarily paused for Board review.

After its review, the ICANN Board expressed concerns that the policy recommendation language did not contain a specific rationale for Recommendation 18 and left the timeline for urgent requests for data disclosure to be worked out in implementation. The Board subsequently concluded that it was necessary to revisit policy recommendation 18 concerning requests for registrant data made in the context of situations that pose an imminent threat to life, serious bodily harm, infrastructure, or child exploitation. Following its review and discussion with the community, the Board noted in its 11 February 2024 correspondence that it would like to avoid further delay of the implementation of the Registration data Policy and "believes that all parties are in agreement with publishing the Registration Data Policy and removing the language on urgent requests for disclosure." As a result, the Registration Data Policy was published on 21 February 2024 without provisions related to the requirements for consideration of and responses to urgent requests.

As part of recommendation 18's further review, in its 3 June 2024 correspondence, the Board identified the concern that urgent requests would more appropriately be addressed within minutes or hours rather than the previously proposed business days, specifically:

> *To the extent that law enforcement needs registration data to respond to situations that pose an imminent threat to life, serious bodily harm, infrastructure, or child exploitation, the* ***proposed timeline - whether one, two, or three business days - does not appear to be fit for purpose. To respond to truly imminent threats, a much shorter response timeline, i.e., minutes or hours rather than days, would seem to be more appropriate****.*

The GAC and GNSO Council also acknowledged that the use of business days does not seem appropriate to respond to Urgent Requests for the disclosure of data..

To address the Board's concern that the use of business days is not fit for purpose to address truly imminent threats and the lack of an authoritative, legally sufficient cross-border system to validate law enforcement entities, on 15 October 2024 the GAC proposed two separate parallel tracks:

1. An authentication path where the GAC PSWG in collaboration with contracted parties explore possible ways forward on an authentication solution.
2. A response time path that focused on the assumption that urgent requests received by registrars have been authenticated.

Subsequently, the GNSO Council, GAC, and ICANN Board held two trilateral calls, where during its 19 December 2024 meeting, the GNSO Council considered the IRT's previous discussions regarding the separate timeline for urgent requests and noted the IRT could not agree to a timeline, in part, because of the lack of a global authentication mechanism.

In light of the GAC's two track proposal to develop such a mechanism, and resume timeline discussions within the EPDP Phase 1 IRT, the Board, GNSO Council, and GAC reached an agreement during their second trilateral meeting on 12 February 2025 to resume implementation work on Recommendation 18 of the EPDP Phase 1 Final Report, specifically related to identifying an appropriate timeline to respond to urgent requests for lawful disclosure. On 27 March 2025, the GNSO Council further acknowledged and agreed with the GAC's suggestion that the discussion regarding the response time for urgent requests should continue within the EPDP - Temp Spec Phase 1 Implementation Review Team, and subsequently asked that ICANN org resume IRT meetings in the near term.

Overview of Urgent Request IRT Discussions and Concerns Raised

ICANN org held a series of IRT sessions to discuss the timeline related to Urgent Requests. Initially ICANN org proposed timeline language to the IRT for consideration on 16 April 2025, specifically:

1. *For Urgent Requests for Lawful Disclosure from an authenticated entity, Registrar and Registry Operator MUST acknowledge receipt of an Urgent Request for Lawful Disclosure* ***without undue delay, but no more than two hours from receipt.***

2. *Following acknowledgement of the Urgent Requests for Lawful Disclosure, Registrars and Registry Operators MUST consider the request on its merits, considering the specific rationale and basis for each request.*

3. *Following its consideration, Registrars and Registry Operators MUST provide its response to the authenticated entity* ***within 24 hours.***

4. *In the event that the Registrar or Registry Operator denies disclosing the data to the requesting authenticated entity, Registrar and Registry Operators MUST provide a rationale for why Registry Operator or Registrar cannot provide the requested data (in whole or in part) that identifies the specific reason(s) for such denial, including a clear explanation of how it arrived at its decision that is sufficient for a requestor to objectively understand the reasons for the decision.*

Urgent Requests IRT Discussion 1

The language received pushback from several IRT members which prompted the following sessions to discuss and understand the concerns the IRT may have when considering a response time of 24 hours.

The initial IRT call focused on updates regarding the urgent request response time, which led to required IRT discussions on a proposed timeline. These discussions centered on the authentication of law enforcement entities that submitted urgent requests and the corresponding response timelines from contracted parties. A key change in the urgent requests discussion is the new caveat: in order for the specific timeline for responses to urgent requests to apply, the request must come from a law enforcement authority that has been authenticated by a to-be-determined mechanism under discussion in the parallel track.
While some IRT members viewed this authentication of identity (once a mechanism is agreed and implemented) as a reason for automatic data release within a matter of seconds or minutes, contracted parties stressed that authentication is only the first step in reviewing the request before determining whether or not to release the data. In addition to authentication, contracted parties

emphasized the need to evaluate the jurisdiction of the requesting law enforcement entity and whether the request meets the defined criteria, such as threats to life, child exploitation, or critical infrastructure. Ultimately, contracted parties require the necessary time to review the request on its merits before making a final decision on whether to release the data or not. GAC IRT members acknowledged the need to review the request and their willingness to work with contracted parties during the review process, with the caveat that law enforcement entities will not disclose specific details of the investigation. As a compromise, GAC members also suggested including in their request an attestation of jurisdiction details and specifying which criterion the urgent request fits under.

Lastly, ICANN org discussed the proposed language, and suggested a potential compromise: the acknowledgment of urgent requests for lawful disclosure must be required within two hours and contracted parties must respond to such requests within 24 hours of receipt. In ICANN org's view, this compromise aligns with the ICANN Board's and GNSO Council's shared expectation that urgent requests should be handled within hours rather than business days. At the same time, contracted parties proposed to revisit the same language proposed in the IRT in July 2023, which provides the opportunity to respond to urgent requests within 24 hours, including a two-business-day extension and an additional business day for complex requests. The registrar IRT members said that this extra time allows contracted parties to conduct further review of the request if needed.

Urgent Requests IRT Discussion 2

Following the first IRT discussion, the IRT was asked to respond to a set of questions aimed at clarifying support for ICANN org's proposal, particularly focusing on whether 24 hours is considered the same as one calendar day, whether measuring an urgent request response time in another unit than business days remains consistent with the intent of EPDP Phase 1 recommendation 18, and inquiring about what additional assurances contracted parties would need to respond to an urgent request from an authenticated law enforcement agent within 24 hours. Specifically, the following questions were circulated to the IRT for a response:

1. *The ICANN Board expressed that responses to Urgent requests should be provided in minutes or hours and the GNSO Council expressed business days is not appropriate. Do IRT members agree that if 24 hours equates to 1 calendar day, then a response to an urgent request cannot take longer than 24 hours and cannot be in business days?*

2. *Do IRT members agree that a timeline to respond to an urgent request measured in another unit than business days can be implemented consistent with Recommendation 18 ?*

3. *Taking into consideration that specifics about the investigation will not be provided, what additional overarching requirements do contracted parties need to quickly review an urgent request and minimize the amount of time needed to provide a response?*

4. *If an authenticated entity submits a request that specifies its jurisdiction and asserts that the urgent request falls under categories such as imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation, is that sufficient to provide a response to the requester within 24 hours?*

GAC IRT members agreed that 24 hours is an appropriate timeframe to respond to an urgent request when considering the exceptional circumstances underpinning urgent requests and the vital public safety interests related to them. However, other IRT members suggested the need for additional data to explain why 24 hours suffices to respond to an urgent request, and they also noted that the 24-hour response time is too long for truly urgent requests, which contracted parties should ideally respond to within minutes or seconds. They further questioned the need for contracted parties to have time to review the request further, provided the law enforcement entity has been authenticated and the request itself includes an attestation to the entity's jurisdiction, as well as which defined criteria the urgent request fits under.

GAC and other IRT members agreed that using a unit outside of business days aligns with the intent of EPDP recommendation 18, as the recommendation itself leaves the timeline flexible for the IRT. These IRT members contended that defining and measuring a required response time for urgent requests in "days" would undermine the concept of an "urgent request".

ICANN org distributed the specific questions above to guide and focus the discussion toward alignment on areas of commonality. However, several IRT members raised other concerns about designing the authentication mechanism, as well as the submission of requests, together with the timeline discussions. These IRT members argued that urgent request timelines cannot be determined in isolation from how the requester will be authenticated and how the request itself will be submitted and received.

Additionally, some members expressed concern that submission mechanisms must remain nonpublic to prevent abuse or manipulation of the urgent request process. Registrar IRT members emphasized that registrars, especially smaller ones, face significant liability if they release user data without a thorough review, even in time-sensitive situations. Therefore, publicizing how to submit an urgent request could lead to system abuse and an increase in misclassified requests. Further, registrar IRT members emphasized that even if a request is authenticated, this doesn't automatically protect registrars from legal consequences, especially across various jurisdictions.

While CPH IRT members also noted that their current practices often align with and exceed response expectations, GAC IRT members stressed the need for codifying these practices into a consensus policy to help standardize such practices. In the GAC IRT members' view, the previously proposed language, which could stretch a response time to four to five days, is not acceptable when dealing with the nature of urgent requests.

Ultimately, both IRT discussions highlighted key areas of divergence within the team. These included the speed at which responses should be delivered, the necessity for additional data collection to justify the inclusion of urgent request response times into a consensus policy, and questions surrounding the scope of the current exercise. In response, ICANN org staff continued to reference the request from the GNSO Council to hold the Urgent Request timeline discussion within the EPDP Phase 1 IRT, which stemmed from the GAC's proposal to have the two separate parallel tracks (namely, 1. Authentication mechanism track, and 2. Timeline discussion track) to address the Urgent Request issue. Additionally, IRT members discussed whether submission and authentication

mechanisms should be defined prior to establishing a timeline, as well as whether the authentication of law enforcement entities removes data holders of legal liability when releasing information.

Both discussions did also identify points of alignment, where IRT members agreed that true urgent requests are rare, but when they do happen, they must be addressed quickly. There was also a general consensus on the need to support law enforcement agencies in life-threatening and time-sensitive situations, emphasizing the importance of developing a practical, secure, and abuse-resistant process.

Urgent Requests IRT Discussion 3 (ICANN 83)

To address the concerns raised in both IRT discussions and in an effort to move the conversation forward, ICANN org circulated a new series of pointed questions to the IRT in preparation for ICANN 83. These questions focused primarily on understanding current practices (including the average response time among contracted parties when handling urgent requests) and identifying the key points that influence those timelines. Additionally, they sought to identify the challenges law enforcement agencies face when submitting urgent requests, and explore what additional safeguards contracted parties might need to ensure consistent responses within 24 hours, while also inviting suggestions for solutions to overcome these obstacles. Specifically:

1. For contracted parties currently responding to urgent requests, what has been the average turnaround time and what factors influence the timeframe?
2. For LEA submitting Urgent Requests, what problems or gaps exist in the current approach?
3. What additional safeguards are needed to confidently commit to respond to an Urgent Request from an authenticated entity within 24 hours?
4. Assuming safeguards and confidentiality are in place, are there any other obstacles that contracted parties might face in consistently providing a response to an urgent request within 24 hours? What practical solutions can be proposed to address these obstacles?

During the discussion at ICANN83, contracted parties noted that they generally do not track the volume of urgent requests they receive, especially given that a centralized system to receive such requests does not exist. They emphasized that there is no "one size fits all" approach to handling urgent requests across registrars. Contracted parties also reiterated that truly urgent requests are relatively rare. For example, Namecheap reported receiving 23 self-identified urgent requests via the Registration Data Request Service (RDRS), of which only one met the criteria to justify a 24-hour turnaround.

Some IRT members also emphasized the importance of clarifying what is considered a "response," noting that a response does not necessarily mean the release of data; it could also involve seeking additional information to evaluate further whether disclosure is appropriate.

When considering the gaps in the current process for law enforcement agencies, GAC members highlighted that the lack of consensus policy around urgent requests creates a policy gap that these

discussions are attempting to address. Some GAC representatives further emphasized that access to registrant contact information has been particularly useful in carrying out abuse victim notifications and other time-sensitive public safety efforts.

Additionally, when discussing what additional safeguards are needed to help contracted parties meet a 24-hour response timeline, many echoed concerns raised in previous IRT meetings. These included the need to verify the jurisdiction of the law enforcement officer as part of the GDPR's balancing test, the ability to conduct internal due diligence when evaluating requests, confirmation that a request truly meets the definition of "urgent," and the possibility of needing additional time in extenuating circumstances, such as when legal input is required to make a data disclosure decision. Further clarification was also provided around the scope of ICANN's remit with respect to enforcement of disclosure-related requirements, including that ICANN policies do not supersede local laws, nor does ICANN compliance review the results of disclosure decisions rendered by the contracted parties.

IRT Urgent Request Proposed Language

In light of these ongoing concerns and the need to balance the necessity of a quick response time while allowing the time for thoughtful review, the Registrar Stakeholder Group, Registries Stakeholder Group and GAC submitted the following Urgent Request response time proposals for IRT consideration:

Registrar Stakeholdergroup Propsal

The Registrar Stakeholder Group proposed the following language that defines an "authenticated entity" and suggests responding to urgent requests generally within 24 hours of receipt, provided the request falls within the relevant jurisdiction of the contracted party and meets the criteria for what constitutes an urgent request. Additionally, the proposal includes an extension of up to three business days for complex or exceptional circumstances. This allows for an additional two business days for exceptional cases and an extra business day for complex requests. The proposal also offers contracted parties the option to request more information about the request to help determine whether to provide the requested data.

> *Definition of Authenticated Entity> "Authenticated Entity" means a law enforcement entity that is authenticated under the process to be determined by a joint GAC and CPH Group working on the issue.*
>
> *10.6. For Urgent Requests for Lawful Disclosure, submitted by an Authenticated Entity, meeting the definition of Urgent requests, and falling within the relevant jurisdiction of the Registrar or Registry Operator, Registrar and Registry Operator MUST respond, as defined in Section 10.7, without undue delay, generally within 24 hours of receipt.*
>
> > *10.6.1. If Registrar or Registry Operator cannot respond to an Urgent Request for Lawful Disclosure within 24 hours, it MUST notify the requestor within 24 hours of receipt of an Urgent Request for Lawful Disclosure of the need for an extension to respond. Registrar or Registry Operator's extension notification to the requestor MUST include (a) confirmation that it has reviewed and considered the Urgent*

Request for Lawful Disclosure on its merits and determined additional time to respond is needed, (b) rationale for why additional time is needed, and (c) the time frame in which it will respond, as required by Section 10.7, which cannot exceed two (2) business days.

10.6.2. In addition to the extension provided for in Section 10.6.1, if responding to an Urgent Request for Lawful Disclosure is complex or a large number of requests are received by Registrar or Registry Operator, it MAY extend the time for response up to an additional one (1) business day provided it notifies the requestor within (2) business days from the time of the initial receipt of the request of the updated time frame to respond explaining the need for an additional extension of time.

10.7.3 Provide a request for further information which is necessary in order to make a decision to provide or not provide the requested data.

GAC Proposal

The GAC, in response to the concerns raised by the registrars, proposed the following language, which includes a designated point of contact to receive urgent requests and the option to request a 72-hour extension to respond to an urgent request for exceptional circumstances:

1. *Registrar and Registry Operators MUST establish and maintain a dedicated point of contact, including a dedicated email address, to receive Urgent Requests for Lawful Disclosure, and MUST provide this contact information to ICANN for the purpose of maintaining a list of such contacts. For Registrar operators, this contact MAY be the same as that described in RAA 3.18.3, which describes "dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity ".*

2. *For Urgent Requests for Lawful Disclosure from an authenticated entity, Registrar and Registry Operator MUST acknowledge receipt of an Urgent Request for Lawful Disclosure* ***without undue delay, but no more than two hours from receipt.***

3. *Following acknowledgement of the Urgent Requests for Lawful Disclosure, Registrars and Registry Operators MUST consider the request on its merits, considering the specific rationale and basis for each request, which may include taking into account jurisdictional issues.*

4. *Following its consideration, Registrars and Registry Operators MUST provide its response to the authenticated entity* ***within 24 hours.***

5. *If exceptional circumstances occur, Registrars and Registry Operators MUST, without undue delay and in all cases within 24 hours, notify the authenticated entity if there is a need for an extension to respond. The notification must include the rationale for the extension and the timeframe within which the Registrar or Registry Operator expects to respond, which cannot exceed* ***72 hours from receipt of the request****. Examples of exceptional circumstances include events of force majeure (unforeseen and uncontrollable events), such as those affecting the availability of the infrastructure, and circumstances associated with the complexity of the*

request, such as a request involving a high number of domain names. For the avoidance of doubt, circumstances which do not justify an extending the 24-hour timeline include foreseeable circumstances such as calendar holidays, planned leave, or planned travel.

6. *In the event that the Registrar or Registry Operator denies disclosing the data to the requesting authenticated entity, Registrar and Registry Operators MUST provide a rationale for why Registry Operator or Registrar cannot provide the requested data (in whole or in part) that identifies the specific reason(s) for such denial, including a clear explanation of how it arrived at its decision that is sufficient for a requestor to objectively understand the reasons for the decision.*

Registries Stakeholder Group Proposal

As part of their proposal, the Registries Stakeholder Group expressed that the rigour associated with authenticating law enforcement agencies through an established authentication system is sufficient to respond to urgent requests within 24 hours. Therefore, they proposed the following language indicating that no additional requirements are necessary:

1. *For Urgent Requests for Lawful Disclosure from an authenticated LEA entity via the approved authentication system, Registrar and Registry Operator MUST acknowledge receipt of an Urgent Request for Lawful Disclosure without undue delay, but no more than two hours from receipt.*

    a. *For avoidance of doubt, Urgent Requests received from an authenticated LEA entity via the approved authentication system will be defined as requests that are limited to circumstances that pose an imminent threat to life, of serious bodily injury, to critical infrastructure, or of child exploitation in cases where disclosure of the data is necessary in combatting or addressing this threat. Critical infrastructure means the physical and cyber systems that are vital in that their incapacity or destruction would have a debilitating impact on economic security or public safety.*

2. *Following acknowledgement of the Urgent Requests for Lawful Disclosure, Registrars and Registry Operators MUST consider the request on its merits, considering the specific rationale and basis for each request.*

3. *Following its consideration, Registrars and Registry Operators MUST provide its response to the LEA authenticated entity within 24 hours.*

4. *In the event that the Registrar or Registry Operator denies disclosing the data to the requesting LEA authenticated entity, Registrar and Registry Operators MUST provide a rationale for why Registry Operator or Registrar cannot provide the requested data (in whole or in part) that identifies the specific reason(s) for such denial, including a clear explanation of how it arrived at its decision that is sufficient for a requestor to objectively understand the reasons for the decision.*

Rationale for New August 2025 ICANN Org Proposed Urgent Request Language

ICANN org held a fourth IRT call on 6 August 2025, where the IRT provided feedback and input on the three proposals received from the GAC, RrSG, and RySG. ICANN org considered all the feedback and input received during the IRT session and as a result proposed the below language based on that feedback. ICANN org's 28 August 2025 proposal includes the definition of Authenticated Requester which states:

> *"Authenticated Requestor" means a law enforcement requestor that is authenticated under the process established and implemented by ICANN in consultation with the ICANN Community; Alternatively, if Registrar or Registry Operator has adopted its own authentication process, an LEA that is authenticated through such an established process.*

Followed by a new Section 10.7 under Disclosure Requests which reads as follows:

10.7 Section 10.7 applies to Urgent Requests. Unless explicitly modified in this Section, all requirements in Section 10 apply equally to Urgent Requests.

> *10.7.1 A Disclosure Request is an Urgent Request if it is submitted by an Authenticated Requestor and such entity attests that the request pertains to at least one of the following circumstances:*
>
> > *10.7.1.1 imminent threat to life*
> > *10.7.1.2 imminent threat of serious bodily injury*
> > *10.7.1.3 imminent threat to critical infrastructure*
> > *10.7.1.4 child exploitation*
>
> *10.7.2 Upon receipt of an Urgent Request, Registrar and Registry Operator MUST:*
> > *10.7.2.1 Acknowledge receipt of the Urgent Request within two hours; and*
> >
> > *10.7.2.2 Respond to the Urgent Request without undue delay, and generally within 24 hours; or*
> >
> > *10.7.2.3 If exceptional circumstances occur, Registrars and Registry Operators MUST, without undue delay and in all cases within 24 hours, notify the Authenticated Requestor if there is a need for an extension to respond. The notification MUST include the rationale for the extension and the timeframe within which the Registrar or Registry Operator expects to respond, which cannot exceed [72 hours from receipt of the request.] Examples of exceptional circumstances include events of force majeure (unforeseen and uncontrollable events), such as those affecting the availability of the infrastructure, and circumstances associated with the complexity of the request, such as a request involving a high number of domain names. For the*

> *avoidance of doubt, circumstances which do not justify extending the 24-hour timeline include foreseeable circumstances such as calendar holidays, planned leave, or planned travel.*

The proposal updates the Urgent Request definition to make clear that Urgent Requests (as defined) are a subset of Disclosure Requests that are subject to a compressed timeline for a required response in addition to all of the other policy requirements that apply to all other Disclosure Requests.. Furthermore, a definition of Authenticated Requestor is proposed to be contingent on the outcome of the parallel effort to agree upon an authentication mechanism. As drafted, the proposal would attach requirements to respond to Urgent Requests for all contracted parties when a mechanism has been implemented to identify Authenticated Requestors.

The IRT previously suggested incorporating "Authenticated LEA entity" within the Urgent Request definition, but ICANN org identified challenges with defining Urgent Requests in this way before a mechanism has been implemented to authenticate requestors. ICANN org believes this approach could unduly limit the Policy language's scope with respect to which requestors may be authenticated under the to-be-agreed and implemented authentication mechanism in the future. Therefore, ICANN org proposes to define "Authenticated Requestor" separately to allow for flexibility in implementation that can adapt to the outcome of authentication-related efforts. Lastly, ICANN org determined that the term "Requestor" provides more clarity on who will be requesting an Urgent Request while the term "entity" provides more ambiguity on who will be submitting such request.

In the current proposal ICANN org assumes that the Authenticated Requestor has done its due diligence to be verified through an external system currently being developed by the GAC PSWG. In light of discussions within the IRT, the definition proposed for Authenticated Requesters would be limited to "law enforcement". However, ICANN org notes that this language could be further future-proofed by removing references to "law enforcement" in the definition of "Authenticated Requestor" to accommodate the possibility that at some future point in time, the community may determine that other types of requestors can and should also be permitted to become "Authenticated." Even with this limitation in the definition removed, the types of requestors that could be authenticated would be limited by the mechanism implemented for authentication. So, if the outcome of the parallel-track work only concerns authentication for law enforcement entities, those would be the only entities that would be eligible to submit Urgent Requests per this proposed Policy language.

The draft policy language proposed would require that Registrars or Registry Operators **acknowledge an urgent request from an authenticated law enforcement entity within two hours from receipt and provide a response to the request within 24 hours of receipt.**

> Some IRT members argued that the method of receiving the request determines how quickly the request will be acknowledged and should be considered alongside the timeline, while others suggested that acknowledgement should take place within a matter of seconds or minutes, as it should be an automatic response. While this is the ideal scenario, the policy recommendations do not suggest the automation of disclosure responses, nor does ICANN

org determine the business models of contracted parties. The timeframe for when the contracted parties acknowledge receipt can take place at any time within the initial two hours of receipt. This allows the flexibility for those who are able to respond immediately to do so, while also providing more time for those who need to acknowledge a request within two hours. Furthermore, the assignment from the GNSO Council and ICANN Board requested that the IRT maintain a limited scope of work, focusing solely on the timeline for responding to urgent requests. The scope of work does not require the IRT to determine the method of receiving the request; the policy recommendation itself also does not require the IRT to determine the method of request. Therefore, this is considered out of scope for the IRT.

ICANN org also notes that LEA have suggested that knowing that the contracted party received the request through a simple acknowledgement is helpful in knowing the request is being worked on. Furthermore, ICANN org clarifies that responding to a request does not necessarily mean that a decision has been made or that the requested data must be provided. A 24-hour response time simply requires a response which not only allows for the requested data to be provided but also allows for the denial of the request, the response that more time is required to review the request, or a response requiring more information prior to deciding on whether or not to provide the requested data. Furthermore, ICANN org ICANN concluded that the term “generally” adds unintended ambiguity on the requirement to respond to an urgent request within 24 hours. ICANN understands that the intent of the requirement is for contracted parties to respond within 24 hours, absent the limited case of an exceptional circumstance, explicitly provided for in section 10.7.3. As including "generally" will limit enforcement of a 24-hour response requirement (for more than the cases that fall under the exception in 10.7.3), and based on a majority view within the IRT, ICANN has removed this from the requirements language. ICANN org understands that in previous iterations, the draft language included the term "generally." This was not previously flagged, as the prior language afforded contracted parties much more leeway to extend the response deadline. This language also preceded the trilateral discussions between the GAC, ICANN Board and GNSO concluding that the response time should be reconsidered by the IRT and specific input from the Board that "a much shorter response timeline, i.e., minutes or hours rather than days, would seem to be more appropriate...

Alternatively, the GAC proposal included an approach for receiving Urgent Requests, which would require contracted parties to establish and maintain a dedicated point of contact. This point of contact may be the same as the one used for receiving reports of illegal activity. Additionally, the GAC proposal would also require contracted parties to share their dedicated contact information with ICANN.

However, ICANN has chosen not to incorporate the GAC's proposal into proposed policy language, as it believes it falls outside the scope of the assignment given by the GNSO Council and the ICANN Board, where the task at hand is to identify a timeline, not to determine the method for receiving Urgent Requests. Furthermore, the IRT also noted that the proposed language addresses an operational gap which should be considered in future work when developing and implementing an authentication system. Furthermore, EPDP recommendation 18 does not ask for how the requests will be received to be considered and

developed during implementation. Instead, Recommendation 18 asks for the consideration of a response time to Urgent Requests for Lawful Disclosure further suggesting that the language proposed by the GAC remains outside of scope for the timeline assignment. Acknowledging that this remains an operational gap that has been discussed in the IRT on numerous occasions, ICANN org incorporated a version of this proposal in an implementation note, indicating that future work on how requirements related to the submission and receipt of Urgent Requests, as well as establishing a contact point for how requests will be submitted, should be determined as part of the authentication mechanism work track.

Another concern raised by contracted parties is the need for flexibility in conducting due diligence when reviewing the request. Given that disclosure requirements described in section 10 of the Registration Data Policy apply to Urgent Requests unless modified by section 10.7, ICANN org believes that Section 10.4 of the Registration Data Policy already requires contracted parties to review disclosure requests on their merits. This allows the contracted party to conduct its review of the request, including confirming that the request falls within the specific criteria of an Urgent Request as well as reviewing the jurisdiction of the law enforcement entity making the request. Thus, considering the request on its merits should suffice in reviewing the request as needed, while also taking into consideration that the GAC specifically stated law enforcement entities will not provide information about the case due to confidentiality reasons, but are willing to work with the registrar if additional information is needed.

In exceptional cases where the contracted party cannot provide a response within 24 hours of receiving the request, the proposal includes the GAC proposal to require contracted parties to notify the Authenticated Requestor if there is a need for an extension to respond to the Urgent Request. The extension must not exceed **72 hours** from receipt of the original request and must contain a rationale and timeframe within which the contracted party expects to respond.

Another concern raised by contracted parties is having the flexibility to consider exceptional cases that may occur and would require a response time longer than 24 hours, such as the need to consult outside counsel prior to providing a response. A compromise requested by the contracted parties was to include the urgent request language that was circulated on 24 July 2023. This proposal includes notifying the requester within 24 hours that the contracted party needs an extension of no more than two business days from the time of the initial receipt of the request as well as an additional business day for complex or large number of requests.

While ICANN org understands that this compromise was close to achieving an agreed-upon timeline for the Registration Data Policy, the maximums included in that proposal, specifically the additional three business days, was noted by the ICANN Board, GAC and GNSO Council as not fit for purpose. As noted above, the Board, GAC, and GNSO Council were aligned in a view that to respond to truly imminent threats, a much shorter response timeline, i.e., minutes or hours rather than days, would seem to be more appropriate. Therefore, ICANN org is not proposing this language for the Registration Data Policy.

In order to consider the concerns raised by the contracted parties, the GAC proposed alternative language as a pathway and flexibility for registrars and Authenticated Requesters to work together, allowing the contracted party to connect with the requestor and communicate the need for an extension with a rationale for why the extension is needed and the expected timeframe of when the request will be addressed.

ICANN org's proposal did not include an additional MAY requirement for contracted parties to request further information which is necessary in order to further determine whether to provide or not provide the requested data. This suggestion was proposed by the Registrar Stakeholder Group who requested the flexibility to inquire for more information from the requestor as needed to help determine whether the requested data should be provided or not. However, ICANN org believes that this suggestion is out of scope because the suggestion was incorporated outside the general timeline update for Urgent Requests. Further contracted parties already have the option to request further information to determine how to respond to an Urgent Request. This option exists in several areas within the existing and proposed policy language. For example, in considering the request on its merits as noted in Section 10.4, contracted parties may request further information based on their review. As noted above, a "response" to an urgent request can also be a request for further information before determining to provide the requested data. Lastly, as noted in the proposed Section 10.7.3, if additional information is needed as part of an exceptional circumstance, contracted parties may communicate this within the allocated 72hour period and update the requestor on its review process as required.

Lastly, the proposal includes an implementation note that further clarifies that contracted parties can continue to utilize their current systems in place to authenticate or validate that an urgent request has been received from an Authenticated Requestor. If they have their own authentication process they may also establish and maintain a designated point of contact to receive an Urgent Request. This clarification was included because there currently is not a standardized authentication mechanism that can currently be enforced on contracted parties to use. Therefore, contracted parties have the option to use their own authentication mechanism until a standardized mechanism is established and implemented by ICANN. The language proposed by ICANN notes that if a contracted party chooses to utilize its own authentication mechanism for urgent requests the timeline requirements in Section 10.7 of the Registration Data Policy Requirements will apply, including the option to establish and maintain a designated point of contact to receive Urgent Requests.

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin.com/company/icann

soundcloud.com/icann

instagram.com/icannorg